

JASON M. WUCETICH (STATE BAR NO. 222113)
jason@wukolaw.com
DIMITRIOS V. KOROVILAS (STATE BAR NO. 247230)
dimitri@wukolaw.com
WUCETICH & KOROVILAS LLP
222 N. Pacific Coast Hwy., Suite 2000
El Segundo, CA 90245
Telephone: (310) 335-2001
Facsimile: (310) 364-5201

MICHAEL S. MORRISON (SBN 205320)
mmorrison@amflp.com
ERIN A. LIM (SBN 323930)
elim@amflp.com
ALEXANDER MORRISON + FEHR LLP
1900 Avenue of the Stars, Suite 900
Los Angeles, CA 90067
Telephone: (310) 394-0888
Facsimile: (310) 394-0811

Attorneys for Plaintiffs
WILLIAM MULLER and ANTONIO KNEZEVICH,
individually and on behalf of all others similarly situated

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

WILLIAM MULLER and ANTONIO
KNEZEVICH, individually and on behalf
of all others similarly situated,

Plaintiffs,

v.

UKG INC.; and DOES 1 through 10,

Defendants.

CASE NO.

CLASS ACTION

COMPLAINT FOR:

- (1) NEGLIGENCE
- (2) NEGLIGENCE PER SE
- (3) UNJUST ENRICHMENT
- (4) DECLARATORY JUDGMENT
- (5) BREACH OF CONTRACT
- (6) VIOLATION OF THE CALIFORNIA
CONSUMER PRIVACY ACT, CAL.
CIV. CODE § 1798.150
- (7) VIOLATION OF THE CALIFORNIA
CUSTOMER RECORDS ACT, CAL.
CIV. CODE § 1798.84
- (8) VIOLATION OF THE CALIFORNIA
UNFAIR COMPETITION LAW,
CAL. BUS. & PROF. CODE § 17200

DEMAND FOR JURY TRIAL

1 Plaintiffs William Muller and Antonio Knezevich (“Plaintiffs”), individually and on
2 behalf of all others similarly situated, hereby complain of defendant UKG Inc. as follows:

3 **SUMMARY OF THE CASE**

4 1. This putative class action arises from defendant UKG Inc.’s negligent failure to
5 implement and maintain reasonable data security procedures and practices, and the consequent
6 massive security breach of its systems that began in December 2021 and remains ongoing as of
7 the date of this complaint. UKG is a multi-billion dollar workforce management technology
8 company that provides third-party human resources services, including timekeeping and payroll
9 services, to companies around the globe. In connection with those services, UKG collects, stores,
10 and processes data for thousands of companies and millions of workers, including a multitude of
11 companies and workers in California and throughout the nation. UKG’s clients form a broad
12 cross section of corporate America and public organizations, including the likes of PepsiCo,
13 Tesla, Gamestop, the University of California system, the County of Santa Clara, and many
14 private and public hospital and healthcare organizations.

15 2. Due to its lack of adequate security measures, UKG suffered a ransomware attack
16 and data breach on or around December 11, 2021. That breach not only exposed millions of
17 workers’ personal information to cybercriminals, but also crippled timekeeping and payroll
18 systems for their employees, resulting in workers whose data was affected not being paid, being
19 paid late, or being paid incorrectly. To compound the matter, the timing of the breach left
20 workers worrying about these financial issues and data concerns in the midst of the holiday
21 season, wondering if they would be able to make ends meet and how long the problem would
22 continue. Those worries proved concrete, as UKG has yet to rectify its security problems and its
23 systems remain disabled as of the date of this complaint.

24 3. Plaintiffs Muller and Knezevich, California PepsiCo and Tesla workers whose data
25 was impacted by the breach and who lost wages as a result, bring this class action complaint to
26 redress these injuries, on behalf of themselves and a nationwide class and California subclass of
27 similarly situated persons. Plaintiffs assert claims on behalf of a nationwide class for negligence,
28 negligence per se, unjust enrichment, declaratory judgment, and breach of contract, as well as

1 claims on behalf of a California subclass for violation of the California Consumer Privacy Act,
2 Cal. Civ. Code § 1798.150, California Customer Records Act, Cal. Civ. Code § 1798.80 *et seq.*,
3 and violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.*
4 Plaintiffs seek, among other things, compensatory damages, punitive and exemplary damages,
5 injunctive relief, attorneys' fees, and costs of suit. Plaintiffs further intend to amend this
6 complaint to seek statutory damages on behalf of the California subclass upon expiration of the
7 30-day cure period pursuant to Cal. Civ. Code § 1798.150(b).

8 **PARTIES**

9 4. Plaintiff William Muller is a citizen and resident of the state of California who
10 works as a truck driver for New Bern Transport Corporation, an exclusive carrier and wholly-
11 owned subsidiary of PepsiCo.

12 5. Plaintiff Antonio Knezevich is a citizen and resident of the state of California who
13 works as a truck driver for Tesla, Inc.

14 6. On information and belief, defendant UKG Inc. is a corporation organized and
15 existed under the laws of the state of Delaware, with dual corporate headquarters in Weston,
16 Florida, and Lowell, Massachusetts.

17 7. Plaintiff is unaware of the true names and capacities, whether individual,
18 association, partnership, corporation, other otherwise, of Does 1 through 10, and therefore sues
19 these defendants by these fictitious names. Each Doe defendant is the principal, agent, or
20 employee of the other and was acting within the scope of such agency or employment to commit
21 the acts alleged herein. Each Doe defendant sued herein aided and abetted the other with the
22 intent that each would be successful in their mutual endeavors. Each Doe defendant contributed
23 to Plaintiffs' damages and the statutory violations alleged herein. Plaintiffs will amend this
24 complaint to allege the Doe defendants' true names and capacities when they become known to
25 Plaintiffs.

26 8. Plaintiffs bring this action on behalf of themselves, on behalf of the general public
27 as a Private Attorney General pursuant to California Code of Civil Procedure § 1021.5 and on
28 behalf of a class and subclass of similarly situated persons pursuant Federal Rule of Civil

1 Procedure 23.

2 **JURISDICTION & VENUE**

3 9. This Court has general personal jurisdiction over UKG Inc. because, at all relevant
4 times, it has had systematic and continuous contacts with the State of California. UKG is
5 registered to do business in California with the California Secretary of State. UKG regularly
6 contracts with a multitude of businesses and organizations in California to provide continuous and
7 ongoing human resources services, including timekeeping and payroll services. And UKG does
8 in fact actually provide such continuous and ongoing human resources services to such companies
9 in California.

10 10. Furthermore, this Court has specific personal jurisdiction over UKG Inc. because
11 the claims in this action stem from its specific contacts with the State of California — namely,
12 UKG’s provision of payroll and other human resource services to a multitude of companies in
13 California, UKG’s collection, maintenance, and processing of the personal data of Californians in
14 connection with such services, UKG’s failure to implement and maintain reasonable security
15 procedures and practices with respect to that data, and the consequent ransomware attack and
16 security breach of such data in December 2021 that resulted from UKG’s failures.

17 11. This Court has diversity subject matter jurisdiction under 28 U.S.C. § 1332(d) in
18 that the matter in controversy exceeds the sum or value of \$5,000,000, exclusive of interests and
19 costs, and is a class action in which members of the class defined herein include citizens of a
20 State different from the defendant. Specifically, defendant UKG Inc. is a citizen of the states of
21 Delaware and/or Florida and/or Massachusetts, and the plaintiff class and/or subclasses defined
22 herein include citizens of other states, including California.

23 12. Venue is proper in the Northern District of California under 28 U.S.C. § 1391
24 (b)(1)-(2) and (c)(2) in that defendant UKG Inc. resides within this judicial district and,
25 alternatively, because a substantial part of the events or omissions giving rise to the claims
26 alleged herein occurred within this judicial district, specifically UKG’s provision of payroll,
27 timekeeping, and other human resource services to a multitude of companies in California,
28 UKG’s collection, maintenance, and processing of the personal data of Californians in connection

1 with such services, UKG's failure to implement and maintain reasonable security procedures and
2 practices with respect to that data, and the consequent ransomware attack and security breach of
3 such data in December 2021 that resulted from UKG's failure. In addition, Plaintiff is informed
4 and believes and thereon alleges that members of the class and subclass defined below reside in
5 the Northern District.

6 **INTRADISTRICT ASSIGNMENT**

7 13. Assignment to the San Francisco/Oakland divisions is proper because a substantial
8 part of the events or omissions which give rise to the claims herein occurred within San Francisco
9 County. Further, pursuant to Civil L. R. 3-2(c), all civil actions which arise in the counties of
10 Alameda, Contra Costa, Del Norte, Humboldt, Lake, Marin, Mendocino, Napa, San Francisco,
11 San Mateo, or Sonoma shall be assigned to the San Francisco/Oakland Divisions. A substantial
12 part of the events or omissions giving rise to the claims herein occurred also within these counties
13 and therefore assignment to the San Francisco/Oakland divisions is proper.

14 **FACTUAL BACKGROUND**

15 14. UKG Inc. (an acronym for Ultimate Kronos Group) is a workforce management
16 technology company with dual headquarters in Florida and Massachusetts that provides human
17 resource services, including timekeeping and payroll services, to a multitude of companies
18 worldwide. The company was founded in April 2020 as the result of a merger between Ultimate
19 Software and Kronos Incorporated. UKG has reportedly been valued at \$22 billion, generates
20 approximately \$3.5 billion in revenue per year, and is one of the largest cloud computing
21 companies in the world. Among other products in its suite of services, UKG provides services
22 known as the "Kronos Private Cloud" and "UKG Workforce Central," which are timekeeping and
23 payroll services.

24 15. UKG provides its timekeeping and payroll services to a multitude of companies
25 and organizations nationwide, including many that operate in California, the likes of which
26 include, are not limited to, PepsiCo, Tesla, Gamestop, the University of California system, the
27 County of Santa Clara, and many private and public hospital and healthcare organizations.
28 UKG's timekeeping and payroll services affect thousands of employers and millions of

1 employees.

2 16. In connection with those services, UKG collects, stores, and processes sensitive
3 personal data for thousands of companies and millions of workers. According to its own privacy
4 policy, available at www.ukg.com/privacy, in connection with its services, UKG collects personal
5 information of individuals from a variety of sources, including directly from its customers and
6 their employees. The privacy policy contains a section entitled “Customers’ Information [and the
7 Information of Their Employees and Job Applicants]”, which states that UKG collects data
8 including, but not limited to “name, company name, address, email address, time and attendance
9 and schedule information, and Social Security Numbers.” On information and belief, UKG also
10 collects banking information in connection with provision of direct deposit payroll processes as
11 well as employee identification numbers. For example, UKG’s website indicates that its services,
12 among other things, allow customers to “[e]nsure accurate, on-time pay to your people” and
13 “[q]uickly generate payroll documents, such as paychecks and direct-deposit files.”¹

14 17. UKG knew that it was a prime target for hackers given the significant amount of
15 sensitive personal information processed through its computer data and storage systems. Experts
16 studying cyber security routinely identify companies such as UKG that collect, process, and store
17 massive amounts of data for other companies as being particularly vulnerable to cyberattacks
18 because of the value of the personal information that they collect and maintain and due to the
19 massive scope of the adverse impact from a breach. UKG’s knowledge is underscored by the
20 massive number of data breaches that have occurred in recent years.

21 18. Despite knowing the prevalence of data breaches, UKG failed to prioritize data
22 security by adopting reasonable data security measures to prevent and detect unauthorized access
23 to its highly sensitive systems and databases. UKG has the resources to prevent a breach, but
24 neglected to adequately invest in data security, despite the growing number of well-publicized
25 breaches. UKG failed to undertake adequate analyses and testing of its own systems, training of
26 its own personnel, and other data security measures to ensure vulnerabilities were avoided or
27 remedied and that Plaintiffs’ and class members’ data were protected.

28 ¹ See <https://www.ukg.com/resources/ukg-pro-pay-product-profile.pdf>.

19. In or around the weekend of December 11, 2021, UKG experienced a massive data security breach as a result of a ransomware attack, which the company disclosed at the beginning of the next week and which was widely reported by the media on December 17, 2021.² The breach impacted, among other things, UKG's "Kronos Private Cloud", which is a data storing device for the company's services, including its timekeeping and payroll services. The breach came after a longstanding security flaw in widely used software across the internet, called Log4j, was made public, opening the door in many companies' systems to hackers. As a result of the security breach, UKG's timekeeping and payroll services were disabled, crippling critical wage payment infrastructure for millions of workers.

20. In addition to payroll issues, the security breach has also resulted in data privacy problems, as the data maintained by UKG includes social security numbers and, on information and belief, banking information. The City of Cleveland announced in a statement after the breach that UKG alerted it that social security numbers of workers may have been stolen in by the hackers inside UKG's network.³

21. On information and belief, the personal information UKG collects and which was impacted by the data breach includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

² See <https://www.cnn.com/2021/12/16/tech/kronos-ransomware-attack/index.html>.

³ See <https://clecityhall.com/2021/12/13/city-of-cleveland-statement-on-ultimate-kronos-group-cybersecurity-incident/>.

1 22. As of the date of this complaint — over a month after the breach — UKG’s
2 systems remain disabled, its systems remain unsecured, and the harm resulting from the data
3 breach remains unrectified.

4 23. Because of the nature of the personal information stored or processed by UKG,
5 Plaintiffs understand that all categories of personal information were subject to unauthorized
6 access and exfiltration, theft, or disclosure. Criminals would have no purpose for hacking UKG
7 other than to exfiltrate or steal the coveted personal information stored or processed by UKG.

8 **Plaintiffs’ Facts**

9 24. Plaintiff William Muller works as a truck driver in California for New Bern
10 Transport Corporation, an exclusive carrier and wholly-owned subsidiary of PepsiCo (New Bern
11 and PepsiCo are collectively referred to herein as PepsiCo). PepsiCo is a client of UKG and
12 utilizes its human resources services, including timekeeping and payroll services, for employees
13 of various entities under the PepsiCo corporate umbrella. In connection with those services,
14 UKG, through PepsiCo, collects, maintains, and processes sensitive personal information of
15 Plaintiff, including, but not limited to, his name, company name, address, e-mail address, time
16 and attendance and schedule information, social security number, employee identification
17 number, and banking information.

18 25. Plaintiff Antonio Knezevich works as a truck driver in California for Tesla, Inc.
19 Tesla is a client of UKG and utilizes its human resources services, including timekeeping and
20 payroll services, for employees. In connection with those services, UKG collects, maintains, and
21 processes sensitive personal information of Plaintiff, including, but not limited to, his name,
22 company name, address, e-mail address, time and attendance and schedule information, social
23 security number, employee identification number, and banking information.

24 26. As a direct and foreseeable result of UKG’s negligent failure to implement and
25 maintain reasonable data security procedures and practices and the resultant breach of its systems,
26 PepsiCo’s and Tesla’s timekeeping and payroll systems became crippled. PepsiCo and Tesla
27 lacked an adequate contingency plan to accurately pay workers, instead relying on UKG to
28 remedy the breach and re-enable its systems. To date, however, that has not occurred. As a stop-

1 gap measure, since the breach PepsiCo and Tesla have adopted a practice of calculating wages
2 due to employees based on, among other things, the averaging of their hours in the weeks prior to
3 the breach. That practice has proved woefully inadequate, resulting in Plaintiffs and employees
4 like Plaintiffs not being fully paid for all time worked, not being paid overtime, being provided
5 inaccurate wage statements or no wage statements at all, not being provided meal and rest breaks
6 or compensation in lieu thereof, all in violation of California law. As but one example, Plaintiffs
7 and other PepsiCo and Tesla drivers worked extensive extra overtime hours since the breach due
8 to it being the busy holiday season. However, PepsiCo's and Tesla's haphazard averaging
9 techniques naturally failed to account for those overtime hours because, among other reasons,
10 they were based on stale data from a less busy season earlier in the year. Accordingly, Plaintiffs,
11 along with other PepsiCo and Tesla employees, have experienced significant monetary loss as
12 consequence of UKG's security breach.

13 27. Members of the class defined herein have similarly experienced significant
14 monetary loss as a result of the security breach because their employers have likewise failed to
15 pay them on time, failed to pay them accurately, or failed to pay them at all due to the crippling of
16 their employers' payroll systems that resulted from the UKG breach.

17 28. As a direct and foreseeable result of UKG's negligent failure to implement and
18 maintain reasonable data security procedures and practices and the resultant breach of its systems,
19 Plaintiffs have also suffered harm in that their sensitive personal information has been exposed to
20 cybercriminals and they has an increased risk and fear of identity theft and fraud. This is not just
21 a generalized anxiety of possible identify theft, privacy, or fraud concerns, but a concrete risk of
22 harm resulting from an actual breach and accompanied by actual instances of reported problems
23 suspect to stem from the breach. In connection with counsel's investigation of this case, workers
24 impacted by the breach, including PepsiCo employees, have reported hacking of their banking
25 information in the weeks following the breach. Twitter users have further reported that as a result
26 of the UKG security breach, hackers obtained workers' phone numbers and began phishing
27 scams. For example, on December 26, 2021, at 1:58 P.M., Twitter user @_genosis_ tweeted:
28 "For all those who have been affected by the Kronos hack please be aware of this. They have

1 already managed to scam a couple hundred employees from another company so be on the look
2 out!” That twitter user posted an image of a text chain stating:

3 Hey Team just a heads up. My sister in law is the HR director [for] Gatorade. They too
4 have been hit by the KRONOS outage. She let me know yesterday that the people that
5 hacked kronos did in fact get employee phone #'s and names. They are now calling
6 PepsiCo/Gatorade employees and saying their work for kronos and are calling to verify
7 employee info. They have managed to scam a couple hundred employees already. Make
8 sure your teams [know] that there is ZERO reason anyone would ever call them and [ask]
9 for their info.

10 Accordingly, Plaintiffs have suffered harm in the form of increased fear and risk of identity theft
11 and fraud resulting from the breach.

12 29. Class members, like Plaintiffs, have also suffered harm in the form of increased
13 risk and fear of identity theft and fraud stemming from the breach. Class members are well aware
14 of the security breach event, as it has impacted their payroll and been widely reported in the
15 media. They are likewise well aware that their sensitive personal information, including social
16 security numbers and potentially banking information, risks being available to other
17 cybercriminals on the dark web.

18 CLASS ACTION ALLEGATIONS

19 30. Plaintiffs bring this action on behalf of themselves and all other similarly situated
20 persons pursuant to Federal Rule of Civil Procedure 23, including Rule 23(b)(1)-(3) and (c)(4).
21 Plaintiffs seek to represent the following class and subclasses:

22 **Nationwide Class.** All persons in the United States whose personal information
23 and/or payroll systems were compromised in or as a result of the data breach of
24 UKG Inc. announced on or around December 11, 2021.

25 **California Subclass.** All persons residing in California whose personal
26 information and/or payroll systems were compromised in or as a result of the data
27 breach of UKG Inc. announced on or around December 11, 2021.

28 Excluded from the class are the following individuals and/or entities: Defendant and its parents,
subsidaries, affiliates, officers, directors, or employees, and any entity in which Defendant has a
controlling interest; all individuals who make a timely request to be excluded from this
proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of

1 this litigation, as well as their immediate family members.

2 31. Plaintiffs reserve the right to amend or modify the class definitions with greater
3 particularity or further division into subclasses or limitation to particular issues.

4 32. This action has been brought and may be maintained as a class action under Rule
5 23 because there is a well-defined community of interest in the litigation and the proposed classes
6 are ascertainable, as described further below:

- 7 a. Numerosity: The potential members of the class as defined are so numerous that
8 joinder of all members of the class is impracticable. While the precise number of
9 class members at issue has not been determined, Plaintiffs believe the security
10 breach affected tens of millions of workers nationwide and at least many tens of
11 thousands within California.
- 12 b. Commonality: There are questions of law and fact common to Plaintiffs and the
13 class that predominate over any questions affecting only the individual members of
14 the class. The common questions of law and fact include, but are not limited to,
15 the following:
- 16 i. Whether UKG owed a duty to Plaintiffs and class members to exercise due
17 care in collecting, storing, processing, and safeguarding their personal
18 information;
 - 19 ii. Whether UKG owed a legal duty to Plaintiffs and class members to
20 exercise due care to avoid sudden disruption of its human resources
21 services, including their timekeeping and payroll services;
 - 22 iii. Whether UKG breached those duties;
 - 23 iv. Whether UKG implemented and maintained reasonable security procedures
24 and practices appropriate to the nature of the personal information of class
25 members;
 - 26 v. Whether UKG acted negligently in connection with the monitoring and/or
27 protecting of Plaintiffs' and class members' personal information;
 - 28

- vi. Whether UKG knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and class members' personal information secure and prevent loss or misuse of that personal information;
- vii. Whether UKG adequately addressed and fixed the vulnerabilities which permitted the data breach to occur;
- viii. Whether UKG caused Plaintiffs and class members damages;
- ix. Whether the damages UKG caused to Plaintiffs and class members include lost wages resulting from the disabling of UKG's timekeeping and payroll services;
- x. Whether the damages UKG caused to Plaintiffs and class members includes the increased risk and fear of identity theft and fraud resulting from the access and exfiltration, theft, or disclosure of their personal information;
- xi. Whether UKG violated the law by failing to promptly notify class members that their personal information had been compromised;
- xii. Whether Plaintiffs and class members are entitled to credit monitoring and other monetary relief;
- xiii. Whether UKG's failure to implement and maintain reasonable security procedures and practices constitutes negligence;
- xiv. Whether UKG's failure to implement and maintain reasonable security procedures and practices constitutes negligence per se;
- xv. Whether UKG's failure to implement and maintain reasonable security procedures and practices constitutes violation of the Federal Trade Commission Act, 15 U.S.C. § 45(a);
- xvi. Whether UKG's failure to implement and maintain reasonable security procedures and practices constitutes violation of the California Consumer Privacy Act, Cal. Civ. Code § 1798.150, California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200; as well as violations of the laws of

the state of Maryland, Delaware, and Florida (the states of which UKG is a citizen), including: the Massachusetts Data Security Statute, Mass. Gen. Laws. Ann. Ch. 93A, §§ 1-2(a), 201 Mass. Code Regs. 17.01-05, the Delaware Computer Security Breach Act, 6 Del. Code Ann. §§ 12B-102, *et seq.*, the Delaware Consumer Fraud Act, 6 Del. Code §§ 2513 *et seq.*, and Florida's Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201 *et seq.*

- xvii. Whether the California subclass is entitled to actual pecuniary damages under the private rights of action in the California Customer Records Act, Cal. Civ. Code § 1798.84 and the California Consumer Privacy Act, Civ. Code § 1798.150, and the proper measure of such damages.
- c. Typicality. The claims of the named Plaintiffs are typical of the claims of the class members because all had their personal information and/or payroll systems compromised as a result of UKG's failure to implement and maintain reasonable security measures and the consequent data breach.
- d. Adequacy of Representation. Plaintiffs will fairly and adequately represent the interests of the class. Counsel who represent Plaintiffs are experienced and competent in consumer and employment class actions, as well as various other types of complex and class litigation.
- e. Superiority and Manageability. A class action is superior to other available means for the fair and efficient adjudication of this controversy. Individual joinder of all Plaintiffs is not practicable, and questions of law and fact common to Plaintiffs predominate over any questions affecting only Plaintiff. Each Plaintiff has been damaged and is entitled to recovery by reason of Defendant's unlawful failure to adequately safeguard their data. Class action treatment will allow those similarly situated persons to litigate their claims in the manner that is most efficient and economical for the parties and the judicial system. As any civil penalty awarded to any individual class member may be small, the expense and burden of individual

litigation make it impracticable for most class members to seek redress individually. It is also unlikely that any individual consumer would bring an action solely on behalf of himself or herself pursuant to the theories asserted herein. Additionally, the proper measure of civil penalties for each wrongful act will be answered in a consistent and uniform manner. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action, as Defendant's records will readily enable the Court and parties to ascertain affected companies and their employees.

33. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the class as a whole.

34. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of the matters and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether UKG owed a legal duty to Plaintiffs and class members to exercise due care in collecting, storing, processing, using, and safeguarding their personal information;
- b. Whether UKG breached that legal duty to Plaintiffs and class members to exercise due care in collecting, storing, processing, using, and safeguarding their personal information;
- c. Whether UKG owed a legal duty to Plaintiffs and class members to exercise due care to avoid sudden disruption of its human resources services, including their timekeeping and payroll services;

- d. Whether UKG breached that legal duty to Plaintiffs and class members to exercise due care to avoid sudden disruption of its human resources services, including their timekeeping and payroll services;
- e. Whether UKG failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;
- f. Whether UKG failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information compromised in the breach; and
- g. Whether class members are entitled to actual damages, credit monitoring, injunctive relief, and/or punitive damages as a result of UKG's wrongful conduct as alleged herein.

FIRST CAUSE OF ACTION

(Negligence, By Plaintiffs and the Nationwide Class Against All Defendants)

35. Plaintiffs reallege and incorporate by reference the preceding paragraphs as if fully set forth herein.

36. UKG owed a duty to Plaintiffs and class members to exercise reasonable care in obtaining, storing, using, processing, deleting and safeguarding their personal information in its possession from being compromised, stolen, accessed, and/or misused by unauthorized persons. That duty includes a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information that were compliant with and/or better than industry-standard practices. UKG's duties included a duty to design, maintain, and test its security systems to ensure that Plaintiffs' and class members' personal information was adequately secured and protected, to implement processes that would detect a breach of its security system in a timely manner, to timely act upon warnings and alerts, including those generated by its own security systems regarding intrusions to its networks, and to promptly, properly, and fully notify its customers, Plaintiffs, and class members of any data breach.

37. UKG's duties to use reasonable care arose from several sources, including but not limited to those described below.

38. UKG had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiffs and class members would be harmed by the failure to protect their personal information because hackers routinely attempt to steal such information and use it for nefarious purposes, but UKG also knew that it was more likely than not Plaintiffs and other class members would be harmed.

39. UKG's duty also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal information by companies such as UKG.

40. Various FTC publications and data security breach orders further form the basis of UKG's duty. According to the FTC, the need for data security should be factored into all business decision making.⁴ In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.⁵ Among other things, the guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach. Additionally, the FTC recommends that companies limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security

⁴ *Start with Security, A Guide for Business*, FTC (June 2015), <https://www.ftc.com/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

⁵ *Protecting Personal Information, A Guide for Business*, FTC (Oct. 2016), https://www.ftc.com/system/files/documents/plain-language/pdf-0136_proteting-personal-informaiton.pdf.

1 measures.

2 41. In addition, individual states have enacted statutes based on the FTC Act that also
3 created a duty, including, among others, those referenced in paragraph 32.b.xvi.

4 42. UKG's duty also arose from its unique position as one of the largest cloud
5 computing companies in the world whose services constitute a linchpin of the payroll services of
6 a substantial fraction of the nation. As set forth above, the data breach herein affected thousands
7 of companies and millions of employees. UKG undertakes its collection of sensitive personal
8 information of employees generally through direct relationships between UKG and employers,
9 generally without the direct consent of employees who have no option but to be affected by
10 UKG's actions. Plaintiffs and class members cannot "opt out" of UKG's activities. UKG holds
11 itself out as a trusted steward of consumer and employee data, and thereby assumed a duty to
12 reasonably protect that data. Plaintiffs and class members, and indeed the general public,
13 collectively repose a trust and confidence in UKG to perform that stewardship carefully.
14 Otherwise consumers and employees would be powerless to fully protect their interests regarding
15 their personal information, which is controlled by UKG. Because of its crucial role within the
16 payroll system, UKG was in a unique and superior position to protect against the harm suffered
17 by Plaintiffs and class members as a result of the UKG data breach. By obtaining, collecting,
18 using, and deriving a benefit from Plaintiffs' and class members' personal information, UKG
19 assumed legal and equitable duties and knew or should have known that it was responsible for
20 protecting Plaintiffs' and class members' personal information from disclosure.

21 43. UKG admits that it has an enormous responsibility to protect employee data, that it
22 is entrusted with this data, and that it did not live up to its responsibilities to protect the personal
23 information at issue here.

24 44. UKG's privacy policy has a specific "Security" section which states:

25 To prevent unauthorized access or disclosure, to maintain data accuracy, and to
26 allow only the appropriate use of your PI, UKG utilizes physical, technical, and
27 administrative controls and procedures to safeguard the information we collect.

28 To protect the confidentiality, integrity, availability and resilience of your PI, we
utilize a variety of physical and logical access controls, firewalls, intrusion

1 detection/prevention systems, network and database monitoring, anti-virus, and
2 backup systems. We use encrypted sessions when collecting or transferring
sensitive data through our websites.

3 We limit access to your PI and data to those persons who have a specific business
4 purpose for maintaining and processing such information. Our employees who
5 have been granted access to your PI are made aware of their responsibilities to
6 protect the confidentiality, integrity, and availability of that information and have
been provided training and instruction on how to do so.

7 Accordingly, UKG admits that it has a duty and responsibility to adequately safeguard Plaintiffs'
8 and class members' personal information.

9 45. UKG also had a duty to safeguard the personal information of Plaintiffs and class
10 members and to promptly notify them and their employers of a breach because of state laws and
11 statutes that require UKG to reasonably safeguard personal information, as detailed herein,
12 including Cal. Civ. Code § 1798.80 *et seq.*

13 46. Timely notification was required, appropriate, and necessary so that, among other
14 things, Plaintiffs and class members could take appropriate measures to freeze or lock their credit
15 profiles, cancel or change usernames or passwords on compromised accounts, monitor their
16 account information and credit reports for fraudulent activity, contact their banks or other
17 financial institutions that issue their credit or debit cards, obtain credit monitoring services,
18 develop alternative timekeeping methods or other tacks to avoid untimely or inaccurate wage
19 payments, and take other steps to mitigate or ameliorate the damages caused by UKG's
20 misconduct.

21 47. UKG also owed a duty to Plaintiffs and class members to exercise reasonable care
22 to avoid sudden disruption of their human resources services, including their timekeeping and
23 payroll services. UKG undertook of its own volition responsibility to provide continuous and
24 ongoing timekeeping and payroll services to the employers of Plaintiffs and class members,
25 knowing that such services were for the benefit of making timely wage payments to them, among
26 other things, and that any disruption, particularly any sudden disruption, would cause Plaintiffs
27 and class members harm.

28 48. Plaintiffs and class members have taken reasonable steps to maintain the

1 confidentiality of their personal information.

2 49. UKG breached the duties it owed to Plaintiffs and class members described above
3 and thus was negligent. UKG breached these duties by, among other things, failing to: (a)
4 exercise reasonable care and implement adequate security systems, protocols and practices
5 sufficient to protect the personal information of Plaintiffs and class members; (b) prevent the
6 breach; (c) detect the breach while it was ongoing; (d) maintain security systems consistent with
7 industry standards and necessary to avoid the disabling of payroll systems for thousands of
8 companies and millions of workers; (e) disclose that Plaintiffs' and class members' personal
9 information in UKG's possession had been or was reasonably believed to have been stolen or
10 compromised; and (f) avoid disruption and continued disruption of its timekeeping and payroll
11 services.

12 50. UKG knew or should have known of the risks of collecting and storing personal
13 information and the importance of maintaining secure systems, especially in light of the
14 increasing frequency of ransomware attacks and known coding vulnerabilities previously reported
15 by news media and Alibaba earlier in 2021. Specifically, among other things, the Log4Shell is a
16 software vulnerability in Apache Log4j 2, a popular Java library for logging error messages in
17 applications. The vulnerability, published prior to the data breach, enables an attacker to take
18 control of a device on the internet if the device is running certain versions of Log4j 2. These
19 vulnerabilities had been reported earlier in 2021. The sheer scope of UKG's operations, which
20 affect thousands of employers and millions of employees, further shows that UKG knew or
21 should have known of the risks and possible harm that could result from its failure to implement
22 and maintain reasonable security measures. On information and belief this is but one of the
23 several vulnerabilities that plagued UKG's systems and led to the data breach.

24 51. Through UKG's acts and omissions described in this complaint, including UKG's
25 failure to provide adequate security and its failure to protect the personal information of Plaintiffs
26 and class members from being foreseeably captured, accessed, exfiltrated, stolen, disclosed,
27 accessed, and misused, UKG unlawfully breached its duty to use reasonable care to adequately
28 protect and secure Plaintiffs' and class members' personal information. UKG further failed to

1 timely and accurately disclose to customers, Plaintiffs, and class members that their personal
2 information had been improperly acquired or access and was available for sale to criminals on the
3 dark web. Indeed, Plaintiffs and class members received no notice of the breach directly from
4 UKG. UKG issued a public statement and in some instances issued notices to its customers (the
5 employers of Plaintiffs and class members) but failed to adequately describe all types of personal
6 information that were exfiltrated, stolen, disclosed, or accessed by the ransomware attackers.

7 52. UKG further breached its duty to Plaintiffs and Class members to exercise
8 reasonable care to avoid sudden disruption of their human resources services, including their
9 timekeeping and payroll services, by allowing its systems to remain disabled for multiple weeks
10 (and counting) and failing to adequately and timely remedy its security vulnerabilities.

11 53. But for UKG's wrongful and negligent breach of its duties owed to Plaintiffs and
12 class members, their personal information would not have been compromised nor their
13 timekeeping and payroll services disabled.

14 54. Plaintiffs and class members relied on UKG to keep their personal information
15 confidential and securely maintained, and to use this information for business purposes only, and
16 to make only authorized disclosures of this information.

17 55. As a direct and proximate result of UKG's negligence, Plaintiffs and class
18 members have been injured as described herein, and are entitled to damages, including
19 compensatory, punitive, and nominal damages, in an amount to be proven at trial. As a result of
20 UKG's failure to protect Plaintiffs' and class members' personal information, Plaintiffs' and class
21 members' personal information has been accessed by malicious cybercriminals. Plaintiffs' and
22 the class members' injuries include:

- 23 a. damages stemming from Plaintiffs and class members not being fully paid for all
24 time worked, not being paid overtime, being provided inaccurate wage statements
25 or no wage statements at all, not being provided meal and rest breaks or
26 compensation in lieu thereof, all in violation of federal and state laws;
- 27 b. damages stemming from the fear and anxiety of Plaintiffs and class members
28 concerning whether they would be fully, timely, and accurately paid for all time

1 worked during the 2021-2022 holiday season, and regarding how long such
2 disruptions to their payroll systems would continue;

- 3 c. theft of their personal information;
- 4 d. costs associated with requested credit freezes;
- 5 e. costs associated with the detection and prevention of identity theft and
6 unauthorized use of their financial accounts;
- 7 f. costs associated with purchasing credit monitoring and identity theft protection
8 services;
- 9 g. unauthorized charges and loss of use of and access to their financial account funds
10 and costs associated with the inability to obtain money from their accounts or
11 being limited in the amount of money they were permitted to obtain from their
12 accounts, including missed payments on bills and loans, late charges and fees, and
13 adverse effects on their credit;
- 14 h. lowered credit scores resulting from credit inquiries following fraudulent
15 activities;
- 16 i. costs associated with time spent and loss of productivity from taking time to
17 address and attempt to ameliorate, mitigate, and deal with the actual and future
18 consequences of the data breach, including finding fraudulent charges, cancelling
19 and reissuing cards, enrolling in credit monitoring and identity theft protection
20 services, freezing and unfreezing accounts, and imposing withdrawal and purchase
21 limits on compromised accounts;
- 22 j. the imminent and certainly impending injury flowing from potential fraud and
23 identity theft posed by their personal information being placed in the hands of
24 criminals;
- 25 k. damages to and diminution of value of their personal information entrusted,
26 directly or indirectly, to UKG with the mutual understanding that UKG would
27 safeguard Plaintiffs' and the class members' data against theft and not allow
28 access and misuse of their data by others;

- 1 l. continued risk of exposure to hackers and thieves of their personal information,
- 2 which remains in UKG's possession and is subject to further breaches so long as
- 3 UKG fails to undertake appropriate and adequate measures to protect Plaintiffs and
- 4 class members;
- 5 m. loss of the inherent value of their personal information;
- 6 n. and other significant additional risk of identity theft, financial fraud, and other
- 7 identity-related fraud in the indefinite future.

SECOND CAUSE OF ACTION

(Negligence Per Se, By Plaintiffs and the Nationwide Class Against All Defendants)

10 56. Plaintiffs reallege and incorporate by reference the preceding paragraphs as if fully
11 set forth herein.

12 57. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair .
13 . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the
14 unfair practice of failing to use reasonable measures to protect personal information by companies
15 such as UKG. Various FTC publications and data security breach orders further form the basis of
16 UKG's duty. In addition, individual states have enacted statutes based on the FTC Act that also
17 created a duty.

18 58. UKG violated Section 5 of the FTC Act (and similar state statutes) by failing to
19 use reasonable measures to protect personal information and not complying with industry
20 standards. UKG's conduct was particularly unreasonable given the nature and amount of
21 personal information it obtained and stored and the foreseeable consequences of a data breach at
22 one of the largest cloud computing companies in the world handling timekeeping and payroll data
23 for thousands of companies and millions of employees.

24 59. UKG's violation of Section 5 of the FTC Act (and similar state statutes)
25 constitutes negligence *per se*.

26 60. Plaintiffs and class members are consumers within the class of persons Section 5
27 of the FTC Act (and similar state statutes) was meant to protect.

28 61. Moreover, the harm that has occurred is the type of harm that the FTC Act (and

similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and the class.

62. UKG is a citizen of the states of Massachusetts, Delaware, and/or Florida, in that it incorporated in Delaware and operates dual headquarters in Massachusetts and Florida. All of its activities are therefore subject to the laws of these states. UKG's actions as described herein constitute unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, in violation of Mass. Gen. Laws. Ann. Ch. 93A, §§ 1-2(a), as well as violations of the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws. Ann. Ch. 93H, § 2; and 201 Mass. Code Regs. 17.01-05, violations of the Delaware Computer Security Breach Act, 6 Del. Code Ann. §§ 12B-102, *et seq.*, the Delaware Consumer Fraud Act, 6 Del. Code §§ 2513 *et seq.*, and violations of Florida's Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201 *et seq.*, specifically in that UKG misrepresented that it would protect the privacy and confidentiality of Plaintiffs and class members' personal information, including by implementing and maintaining reasonable security measures, then failed to do so, and further failed to promptly, fully, and adequately notify Plaintiffs and class members of the breach. UKG's violations of these statutes constitute negligence *per se*. Plaintiffs and class members are within the class of persons these statutes were meant to protect. Moreover, the harm that has occurred is the type of harm that these state statutes intended to guard against.

63. As a direct and proximate result of UKG's negligence, Plaintiffs and class members have been injured as described herein and in paragraph 55 above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION

(Unjust Enrichment, By Plaintiffs and the Nationwide Class Against All Defendants)

64. Plaintiffs reallege and incorporate by reference the preceding paragraphs as though fully set forth herein.

1 65. Plaintiffs and class members have an interest, both equitable and legal, in the
2 personal information about them that was conferred upon, collected by, and maintained by UKG
3 and that was ultimately converted, stolen, removed, deleted, exfiltrated, or disclosed in the UKG
4 data breach. This personal information was conferred on UKG in most cases by third parties,
5 class members' employers, but in some instances directly by Plaintiffs and class members
6 themselves.

7 66. UKG was benefitted by the conferral upon it of the personal information
8 pertaining to Plaintiffs and class members and by its ability to retain and use that information.
9 UKG understood that it was in fact so benefitted.

10 67. UKG also understood and appreciated that the personal information pertaining to
11 Plaintiffs and class members was private and confidential and its value depended upon UKG
12 maintaining the privacy, security, and confidentiality of that personal information.

13 68. But for UKG's willingness and commitment to maintain its privacy, security, and
14 confidentiality, that personal information would not have been transferred to and entrusted with
15 UKG. Further, if UKG has disclosed that its data security measures were inadequate, UKG
16 would not have been permitted to continue in operation by regulators, its shareholders, and
17 participants in the marketplace.

18 69. As a result of UKG's wrongful conduct as alleged in this Complaint (including
19 among other things its failure to employ adequate data security measures, its continued
20 maintenance and use of the personal information belonging to Plaintiffs and class members
21 without having adequate data security measures, and its other conduct in facilitating the theft of
22 that personal information), UKG has been unjustly enriched at the expense of, and to the
23 detriment of, Plaintiffs and class members. Among other things, UKG has and continues to
24 benefit and profit from the sale of the personal information and from its contracts to use that
25 personal information to process timekeeping and payroll, while the value to Plaintiffs and class
26 members has been diminished.

27 70. UKG's unjust enrichment is traceable to, and resulted directly and proximately
28 from, the conduct alleged herein, including the compiling and use of Plaintiffs' and Class

1 members' sensitive personal information, while at the same time failing to maintain that
2 information secure from intrusion and theft by hackers and identity thieves.

3 71. Under the common law doctrine of unjust enrichment, it is inequitable for UKG to
4 be permitted to retain the benefits it received, and is still receiving, without justification, from
5 Plaintiffs and class members in an unfair and unconscionable manner. UKG's retention of such
6 benefits under circumstances making such retention inequitable constitutes unjust enrichment.

7 72. The benefit conferred upon, received, and enjoyed by UKG was not conferred
8 officiously or gratuitously, and it would be inequitable and unjust for UKG to retain the benefit.

9 73. UKG is therefore liable to Plaintiffs and class members for restitution in the
10 amount of the benefit conferred on UKG as a result of its wrongful conduct, including
11 specifically the value to UKG of the personal information that was stolen and the payroll systems
12 that were compromised in the UKG data breach and the profits UKG is receiving from the use,
13 sale, and processing of that information, including any profits from its timekeeping and payroll
14 services.

15 **FOURTH CAUSE OF ACTION**

16 **(Declaratory Judgment, By Plaintiffs and the Nationwide Class Against All Defendants)**

17 74. Plaintiffs reallege and incorporate by reference the preceding paragraphs as though
18 fully set forth herein.

19 75. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 *et seq.*, this Court is
20 authorized to enter a judgment declaring the rights and legal relations of the parties and grant
21 further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here,
22 that are tortious and violate the terms of the federal and state statutes described in this complaint.

23 76. An actual controversy has arisen in the wake of the UKG data breach regarding its
24 present and prospective common law and other duties to reasonably safeguard its customers and
25 their employees' personal information, to avoid disruption of timekeeping and payroll services,
26 and regarding whether UKG is currently maintaining data security measures adequate to protect
27 Plaintiffs and class members from further data breaches that compromise their personal
28

1 information and timekeeping and payroll services. Plaintiffs allege that UKG's data security
2 measures remain inadequate. UKG denies these allegations. Plaintiffs continue to suffer injury
3 as a result of the compromise of their personal information and remain at imminent risk that
4 further compromises of their personal information will occur in the future.

5 77. Pursuant to its authority under the Declaratory Judgment Act, this Court should
6 enter a judgment declaring, among other things, the following:

- 7 a. UKG continues to owe a legal duty to secure consumers' and employees personal
8 information, including Plaintiffs' and class members' personal information, to
9 timely notify them of a data breach under the common law, Section 5 of the FTC
10 Act, and various state statutes, and to avoid disruption to their timekeeping and
11 payroll services;
- 12 b. UKG continues to breach this legal duty by failing to employ reasonable measures
13 to secure Plaintiffs' and class members' personal information and by failing to
14 avoid disruption of their timekeeping and payroll services.

15 78. The Court should issue corresponding prospective injunctive relief requiring UKG
16 to employ adequate security protocols consistent with law and industry standards to protect
17 Plaintiffs' and class members' personal information and timekeeping and payroll services.

18 79. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an
19 adequate legal remedy, in the event of another data breach at UKG. The risk of another such
20 breach is real, immediate, and substantial. If another breach at UKG occurs, Plaintiffs will not
21 have an adequate remedy at law because many of the resulting injuries are not readily quantified
22 and they will be forced to bring multiple lawsuits to rectify the same conduct.

23 80. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to
24 UKG if an injunction is issued. Among other things, if another massive data breach occurs at
25 UKG, Plaintiffs and class members will likely be subjected to substantial identity theft and other
26 damage, including continuing lost wages from timekeeping and payroll interruptions. On the
27 other hand, the cost to UKG of complying with an injunction by employing reasonable
28 prospective data security measures is relatively minimal, and UKG has a pre-existing legal

obligation to employ such measures.

81. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at UKG, thus eliminating the additional injuries that would result to Plaintiffs and the millions of class members whose confidential information would be further compromised.

FIFTH CAUSE OF ACTION

(Breach of Contract, By Plaintiffs and the Nationwide Class Against All Defendants)

82. Plaintiffs reallege and incorporate by reference the preceding paragraphs as though fully set forth herein.

83. UKG's privacy policy is an agreement between UKG and its customers as well as the employees of its customers, who include Plaintiffs and class members, and who provided their personal information to UKG.

84. UKG's privacy policy has a "Security" section which specifically states:

To prevent unauthorized access or disclosure, to maintain data accuracy, and to allow only the appropriate use of your PI, UKG utilizes physical, technical, and administrative controls and procedures to safeguard the information we collect.

To protect the confidentiality, integrity, availability and resilience of your PI, we utilize a variety of physical and logical access controls, firewalls, intrusion detection/prevention systems, network and database monitoring, anti-virus, and backup systems. We use encrypted sessions when collecting or transferring sensitive data through our websites.

We limit access to your PI and data to those persons who have a specific business purpose for maintaining and processing such information. Our employees who have been granted access to your PI are made aware of their responsibilities to protect the confidentiality, integrity, and availability of that information and have been provided training and instruction on how to do so.

85. This privacy policy constitutes a contract or implied contract between UKG, on the one hand, and Plaintiffs and class members, on the other hand. This contract or implied contract was formed when Plaintiffs and Class members entrusted their personal information to their employers, who in turn entrusted it to UKG, and in instances when Plaintiffs and class members provided their personal information directly to UKG. UKG specifically contracted to implement

1 and maintain reasonable security measures and to limit access to Plaintiffs' and class members'
 2 data, and undertook a responsibility and contractual obligation to do so. UKG undertook these
 3 duties specifically for the purpose of facilitating continuing and ongoing payroll and timekeeping
 4 services for Plaintiffs and class members.

5 86. Plaintiffs and class members are further third-party beneficiaries of any such
 6 contract between their employers and UKG.

7 87. Plaintiffs and class members fully performed their obligations under the contracts
 8 or implied contracts with UKG.

9 88. UKG breached its contracts or implied contracts with Plaintiffs and class members
 10 by failing to protect their personal information. Specifically, it failed to take reasonable steps to
 11 use safe and secure systems to protect that information, failed to have appropriate security
 12 protocols and measures in place to protect that information, such as adequate internal and external
 13 firewalls, physical security, technological security measures, and encryption, disclosed that
 14 information to unauthorized third parties, failed to promptly alert or give notice of the breach to
 15 Plaintiffs and class members, and failed to adequately continue to provide ongoing payroll and
 16 maintenance services to Plaintiffs and class members.

17 89. As a direct and proximate result of UKG's breaches of contract, Plaintiffs and
 18 class members sustained actual losses, damages, and consequential damages as described above,
 19 and are also entitled to recover nominal damages.

20 **SIXTH CAUSE OF ACTION**

21 **(Violation of the California Consumer Privacy Act, 22 Cal. Civ. Code §§ 1798.100 *et seq.*, § 1798.150(a) 23 By Plaintiffs and the California Subclass Against All Defendants)**

24 90. Plaintiffs reallege and incorporate by reference the preceding paragraphs as though
 25 fully set forth herein.

26 91. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a),
 27 creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically
 28 provides:

Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than one hundred dollars (\$100) and not greater than seven hundred and fifty (\$750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

92. UKG is a "business" under § 1798.140(b) in that it is a corporation organized for profit or financial benefit of its shareholders or other owners, with gross revenue in excess of \$25 million. Indeed, its revenue reaches into the many billions per year.

93. Plaintiffs and California subclass members are covered "consumers" under § 1798.140(g) in that they are natural persons who are California residents.

94. The personal information of Plaintiffs and the California subclass at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and 1798.81.5, in that the personal information UKG collects and which was impacted by the data breach includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

1 95. UKG knew or should have known that its computer systems and data security
2 practices were inadequate to safeguard the California subclass's personal information and that the
3 risk of a data breach or theft was highly likely. UKG failed to implement and maintain
4 reasonable security procedures and practices appropriate to the nature of the information to
5 protect the personal information of Plaintiffs and the California subclass. Specifically, UKG
6 subjected Plaintiffs' and the California subclass's nonencrypted and nonredacted personal
7 information to an unauthorized access and exfiltration, theft, or disclosure as a result of the
8 UKG's violation of the duty to implement and maintain reasonable security procedures and
9 practices appropriate to the nature of the information, as described herein.

10 96. As a direct and proximate result of UKG's violation of its duty, the unauthorized
11 access and exfiltration, theft, or disclosure of Plaintiffs' and class members' personal information
12 included exfiltration, theft, or disclosure through UKG's servers, systems, and website, and/or the
13 dark web, where hackers further disclosed UKG's customers' and their employees' personal
14 information.

15 97. As a direct and proximate result of UKG's acts, Plaintiffs and the California
16 subclass were injured and lost money or property, including but not limited to lost wages due to
17 the disabling of their payroll and timekeeping services, the loss of Plaintiffs' and the subclass's
18 legally protected interest in the confidentiality and privacy of their personal information, nominal
19 damages, and additional losses described above.

20 98. Section 1798.150(b) specifically provides that "[n]o [prefiling] notice shall be
21 required prior to an individual consumer initiating an action solely for actual pecuniary damages."
22 Accordingly, Plaintiffs and the California subclass by way of this complaint seek actual pecuniary
23 damages suffered as a result of UKG's violations described herein. Plaintiffs have issued and/or
24 will issue a notice of these alleged violations pursuant to § 1798.150(b) and intend to amend this
25 complaint to seek statutory damages and injunctive relief upon expiration of the 30-day cure
26 period pursuant to § 1798(a)(1)(A)-(B), (a)(2), and (b).

SEVENTH CAUSE OF ACTION

**(Violation of the California Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.*,
By Plaintiffs and the California Subclass Against All Defendants)**

99. Plaintiffs reallege and incorporate by reference the preceding paragraphs as though fully set forth herein.

100. Cal. Civ. Code § 1798.81.5 provides that “[i]t is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information.”

101. Section 1798.81.5(b) further states that: “[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.”

102. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a violation of this title may institute a civil action to recover damages.” Section 1798.84(e) further provides that “[a]ny business that violates, proposes to violate, or has violated this title may be enjoined.”

103. Plaintiffs and member the California subclass are “customers” within the meaning of Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided personal information to UKG, directly and/or indirectly through their employers, for the purpose of obtaining a service from UKG.

104. The personal information of Plaintiffs and the California subclass at issue in this lawsuit constitutes “personal information” under § 1798.81.5(d)(1) in that the personal information UKG collects and which was impacted by the data breach includes an individual’s first name or first initial and the individual’s last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social security number; (ii) Driver’s license number, California identification card number, tax identification number, passport number, military identification number, or other unique

1 identification number issued on a government document commonly used to verify the identity of
2 a specific individual; (iii) account number or credit or debit card number, in combination with any
3 required security code, access code, or password that would permit access to an individual's
4 financial account; (iv) medical information; (v) health insurance information; (vi) unique
5 biometric data generated from measurements or technical analysis of human body characteristics,
6 such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

7 105. UKG knew or should have known that its computer systems and data security
8 practices were inadequate to safeguard the California subclass's personal information and that the
9 risk of a data breach or theft was highly likely. UKG failed to implement and maintain
10 reasonable security procedures and practices appropriate to the nature of the information to
11 protect the personal information of Plaintiffs and the California subclass. Specifically, UKG
12 failed to implement and maintain reasonable security procedures and practices appropriate to the
13 nature of the information, to protect the personal information of Plaintiffs and the California
14 subclass from unauthorized access, destruction, use, modification, or disclosure. UKG further
15 subjected Plaintiffs' and the California subclass's nonencrypted and nonredacted personal
16 information to an unauthorized access and exfiltration, theft, or disclosure as a result of the
17 UKG's violation of the duty to implement and maintain reasonable security procedures and
18 practices appropriate to the nature of the information, as described herein.

19 106. As a direct and proximate result of UKG's violation of its duty, the unauthorized
20 access, destruction, use, modification, or disclosure of the personal information of Plaintiffs and
21 the California subclass included hackers' access to, removal, deletion, destruction, use,
22 modification, disabling, disclosure and/or conversion of the personal information of Plaintiffs and
23 the California subclass by the ransomware attackers and/or additional unauthorized third parties
24 to whom those cybercriminals sold and/or otherwise transmitted the information.

25 107. As a direct and proximate result of UKG's acts or omissions, Plaintiffs and the
26 California subclass were injured and lost money or property, including but not limited to lost
27 wages due to the disabling of their payroll and timekeeping services, the loss of Plaintiffs' and the
28 subclass's legally protected interest in the confidentiality and privacy of their personal

information, nominal damages, and additional losses described above. Plaintiffs seek compensatory damages as well as injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).

EIGHTH CAUSE OF ACTION

(Violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code §17200 *et seq.* By Plaintiffs and the California Subclass Against All Defendants)

108. Plaintiffs reallege and incorporate by reference the preceding paragraphs as though fully set forth herein.

109. UKG is a “person” defined by Cal. Bus. & Prof. Code § 17201.

110. UKG violated Cal. Bus. & Prof. Code § 17200 *et seq.* (“UCL”) by engaging in unlawful, unfair, and deceptive business acts and practices.

111. UKG’s “unfair” acts and practices include:

- a. UKG failed to implement and maintain reasonable security measures to protect Plaintiffs and California subclass members’ personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the UKG data breach. UKG failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry, for example the Log4Shell is a software vulnerability in Apache Log4j 2, a popular Java library for logging error messages in applications. UKG failed to patch these and other problems, which made it trivial for a hacker to penetrate UKG’s systems. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiffs and the California subclass, whose personal Information has been compromised.
- b. UKG’s failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers’ data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), California’s Customer Records Act (Cal. Civ. Code § 1798.80 *et seq.*), and

California's Consumer Privacy Act (Cal. Civ. Code § 1798.150).

c. UKG's failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of UKG's inadequate security, consumers could not have reasonably avoided the harms that UKG caused.

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

112. UKG has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumer Privacy Act, Cal. Civ. Code § 1798.150, California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, and California common law.

113. UKG's unlawful, unfair, and deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and California subclass members' personal information, which was a direct and proximate cause of the UKG data breach
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the UKG data breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and California subclass members' personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.*, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150, which was a direct and proximate cause of the UKG data breach.
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and California subclass members' personal information, including by

1 implementing and maintaining reasonable security measures;

- 2 e. Misrepresenting that it would comply with common law and statutory duties
 3 pertaining to the security and privacy of Plaintiffs and California subclass
 4 members' personal information, including duties imposed by the FTC Act, 15
 5 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et*
 6 *seq.*, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150.
- 7 f. Omitting, suppressing, and concealing the material fact that it did not reasonably
 8 or adequately secure Plaintiffs and California subclass members' personal
 9 information; and
- 10 g. Omitting, suppressing, and concealing the material fact that it did not comply with
 11 common law and statutory duties pertaining to the security and privacy of
 12 Plaintiffs and California subclass members' personal information, including duties
 13 imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal.
 14 Civ. Code §§ 1798.80, *et seq.*, and California's Consumer Privacy Act, Cal. Civ.
 15 Code § 1798.150.

16 114. UKG's representations and omissions were material because they were likely to
 17 deceive reasonable consumers about the adequacy of UKG's data security and ability to protect
 18 the confidentiality of consumers' personal information and ongoing provision of timekeeping and
 19 payroll services.

20 115. As a direct and proximate result of UKG's unfair, unlawful, and fraudulent acts
 21 and practices, Plaintiffs and California subclass members were injured and lost money or
 22 property, including the lost wages directly resulting from the disabling of the timekeeping and
 23 payroll systems of the employers of Plaintiffs and subclass members, which would not have
 24 occurred but for the unfair and deceptive acts, practices, and omissions alleged herein, as well as
 25 the costs passed through from UKG to its customers and their employees for their timekeeping
 26 and payroll services, monetary damages from fraud and identity theft, time and expenses related
 27 to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud
 28 and identity theft, and loss of value of their Personal Information, and well as the time and

1 expense of finding alternative methods of timekeeping and payroll services.

2 116. UKG acted intentionally, knowingly, and maliciously to violate California's
3 Unfair Competition Law, and recklessly disregarded Plaintiffs and California subclass members'
4 rights. Past data breaches put it on notice that its security and privacy protections were
5 inadequate.

6 117. Plaintiffs and California subclass members seek all monetary and nonmonetary
7 relief allowed by law, including restitution of all profits stemming from UKG's unfair, unlawful,
8 and fraudulent business practices or use of their personal information; declaratory relief;
9 reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5;
10 injunctive relief; and other appropriate equitable relief, including public injunctive relief.

11 **PRAYER FOR RELIEF**

12 WHEREFORE, Plaintiffs, on behalf of themselves, the nationwide class, and the
13 California subclass, pray for the following relief:

- 14 1. An order certifying the nationwide class and California subclass as defined above
15 pursuant to Fed. R. Civ. P. 23 and declaring that Plaintiffs are proper class
16 representatives and appointing Plaintiffs' counsel as class counsel;
- 17 2. Permanent injunctive relief to prohibit UKG from continuing to engage in the
18 unlawful acts, omissions, and practices described herein;
- 19 3. Compensatory, consequential, general, and nominal damages in an amount to be
20 proven at trial, in excess of \$5,000,000;
- 21 4. Disgorgement and restitution of all earnings, profits, compensation, and benefits
22 received as a result of the unlawful acts, omissions, and practices described herein;
- 23 5. Punitive, exemplary, and/or trebled damages to the extent permitted by law;
- 24 6. A declaration of right and liabilities of the parties;
- 25 7. Costs of suit;
- 26 8. Reasonable attorneys' fees, including pursuant to Cal. Civ. Pro. Code § 1021.5;
- 27 9. Pre- and post-judgment interest at the maximum legal rate;
- 28 10. Distribution of any monies recovered on behalf of members of the Class or the general

1 public via fluid recovery or *cy pres* recovery where necessary and as applicable to
2 prevent Defendant from retaining the benefits of their wrongful conduct; and
3 11. Such other relief as the Court deems just and proper.

4 Dated: January 18, 2022

ALEXANDER MORRISON + FEHR LLP
WUCETICH & KOROVILAS LLP

7
8 By: /s/ Dimitrios V. Korovilas

DIMITRIOS V. KOROVILAS
Attorneys for Plaintiffs
William Muller and Antonio Knezevich,
individually and on behalf of
all others similarly situated

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the putative class and subclass, hereby demands a trial by jury on all issues of fact or law so triable.

Dated: January 18, 2022

ALEXANDER MORRISON + FEHR LLP

WUCETICH & KOROVILAS LLP

By: /s/ Dimitrios V. Korovilas

DIMITRIOS V. KOROVILAS

Attorneys for Plaintiffs

William Muller and Antonio Knezevich,
individually and on behalf of
all others similarly situated